Module 5- Computer Systems (2023-24)

Project

UNIVERSITY
OF TWENTE.

Project Name: Earthquake Detector	Team ID: **Cenk Dogruer s2875144, Cuong Bui Duc s2966174, Hieu Chu s2948923, Rudolfs Neija s2975157, Carlo Fernandes de Brito s2980460**
Team Members: 15	Mentor(s): **Maxim Rosca, Vithursika Vinasiththamby**

Security by Design Checklist

Instructions:

A. **All the sections are mandatory.**
B. **Complete the sections in the below table and put a checkmark if you have done.**
C. **Think about your application and work on the sections accordingly.**
D. **Feel free to add extra requirements for reviewing security architecture and their countermeasures for your application, if needed.**

Sr. No.	Review Security Architecture	Put checkmark ✓ if you have completed the Review Security Architecture as suggested in the left column	Additional comments (If required)	Security Controls/Countermeasures	Put checkmark ✓ if you have completed the Security controls points as suggested in the left column	Additional comments (if required)
1	**Check Trust Boundaries,** identify areas where sensitive data and control mechanisms exist. The accelerometer area is sensitive in case of data manipulation and errors.	✓		To prevent any manipulation and minor changes to the sensors, implementation of a physical case for both manipulation and protection of the device has been aggreed.	✓	
2	**Identify data flows**, processed sensor data, including feature extraction and earthquake event detection. Implement secure data processing to prevent unauthorized access or tampering with data during analysis.	✓		**Check the mitigation criteria to reduce the impact of the risk/threat for the application.** Implement Multi-Factor Authentication (MFA) for privileged accounts and access to sensitive components (address, personal information...), enhancing authentication security.	✓	

3	Entry and Exit points of the system and its components.	√		Make a data flow diagram to visualize and understand the data flow, input, output points, and trust boundary.	√	
4	Write the complete architecture in the SDD template. Review and approve among yourselves and by your assigned mentor(s).	√		Analyze the cost involved to implement the security controls (if any).	√	
	Team members' reviewed:	Carlo Fernandes de Brito: Yes Duc Cuong Bui: Yes Hieu Chu Minh: Yes Cenk Doğruer: Yes Rudolfs Neija: Yes				

Software Design Document Template

Instructions:

i) You must explain all the given sections clearly and concisely.

ii) You must fill in the basic information about your projects such as Project Name, Team Members, Team ID, and Mentor(s).

iii) Make sure to consider the checklist of the Design phase provided in the Security by Design document.

iv) The length of the document should be 4 to 8 pages (including the diagrams).

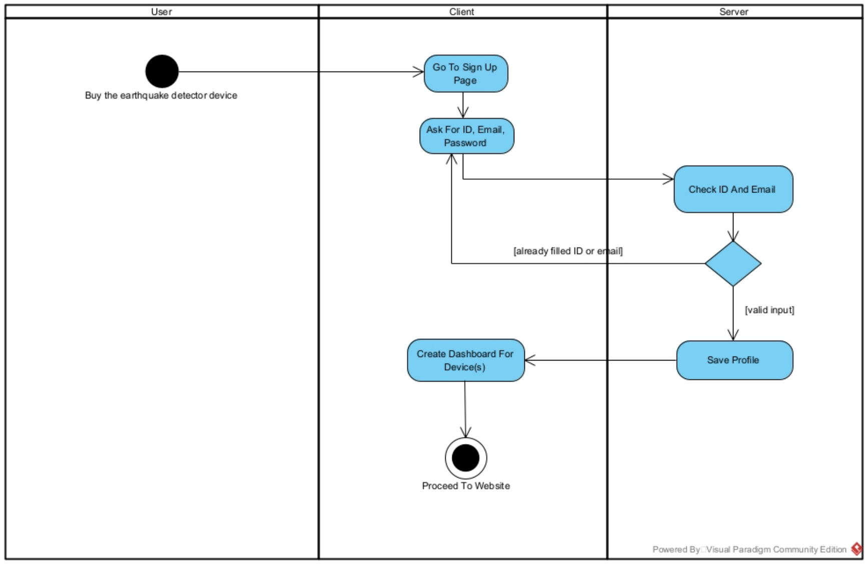
1. Introduction

Welcome to our web application, this application will be an easy way for the user to view their devices and their activity. When accessing the application, they will first be met with a login page were their credentials will be checked. When these are valid, they will be able to do a number of things on the application. A few things that they will be able to do are monitor real life activity, view past readings, set detection profiles, or track the location of their devices. We are making it as user friendly as possible and hope to be able to help the people that use the system.

2. Functional/Non Functional Requirements

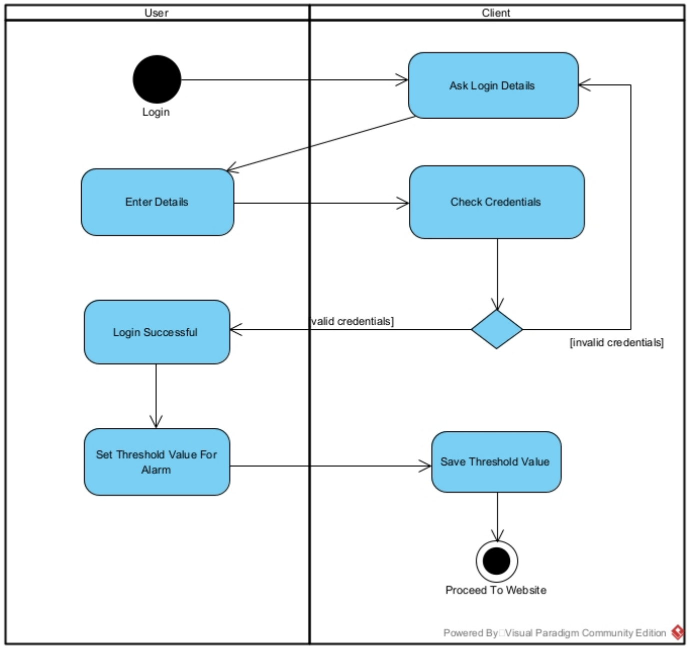
We didn’t change any of the requirements since handing in the resit for the RAD-assignment.

3. Architectural Design


User
Client
Server
Buy the earthquake detector device
Go To Sign Up Page
Ask For ID, Email, Password
Check ID And Email
[already filled ID or email]
[valid input]
Save Profile
Create Dashboard For Device(s)
Proceed To Website
Powered By: Visual Paradigm Community Edition

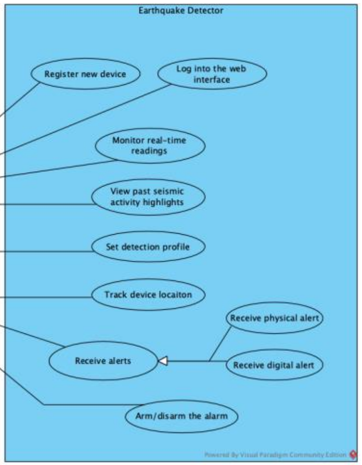
This activity diagram demonstrates how the user will be able to use detector after he/she buys the detector. First, the user buys the detector, and then goes onto the website to sign up. Then, the user puts in the ID of the device which is already included within itself when the user bought the device. After the user signs up with the password, email, and device ID; if the ID or email is not valid, which means that if they are being used by other users, it will be declined, and a new ID and email will be asked. If the credentials are valid, then a dashboard will be created for the user related to their device(s).

Activity Diagram:



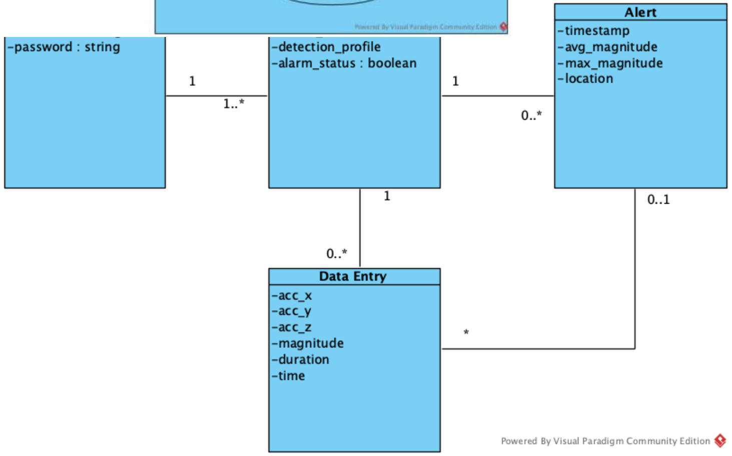
This activity diagram demonstrates how the user will login and it explains how the website is set with its features. First, the website asks for the login details, after the user enters the details, based on the validity of the credentials, website either asks for the login details again or demonstrates that the login is successful and allows the user to set the features based on the users' preferences. After the features are set, the data is kept on the website for further use.

Use Case Diagram:



The use case diagram contains only a single actor because this system will have only one type of user interacting with it, namely the owner/primary user of the device. The user can power arm or disarm the alarm with a hardware switch. They will also be able to receive physical alerts via a light and a speaker, and notifications on the web interface which facilitates most functionality. By registering and/or logging in, the user can view live and past events and see the device's location. They can also select the detection profile, which alters the alarm threshold. This option is for when the user wishes to use the device for other purposes, such as home security, which might require different sensor sensitivity.

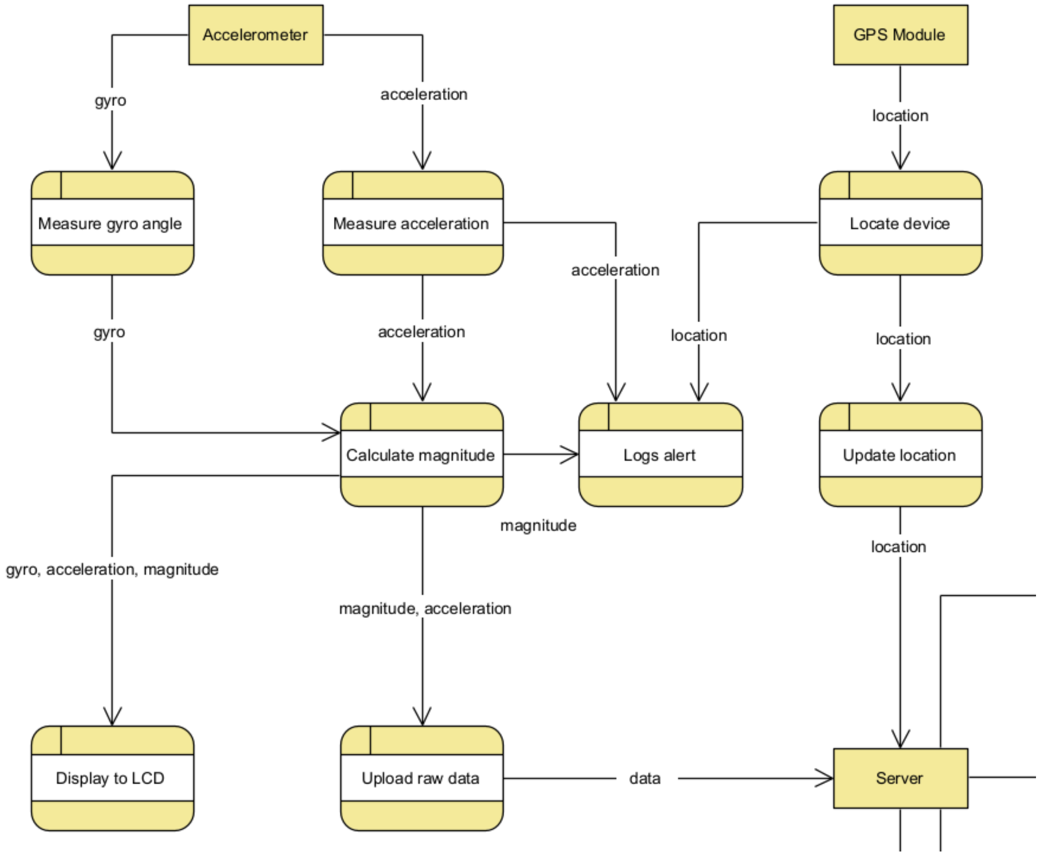
Class diagram:



Each registered user can choose a username and a password. A device has its own unique ID and keeps track of its active detection profile and the alarm status. A device can belong to only one user to help keep sensitive data secure. While in operation, the device periodically generates data entries (since the sensor collects data in discrete steps). Here, the acceleration in each direction is the raw sensor data from which magnitude is calculated. The duration is the duration (size) of the time step. If at any point the detection threshold is exceeded, an alert is generated with a timestamp. The average magnitude is calculated from the past few minutes of data entries as well as entries generated some amount of time in the future. From that same data, the maximum magnitude is recorded as well as the locaiton from the GPS module. The exact time frame for the relevant alert data will be determined in testing. Data entries generated during that time frame will be saved to disk.

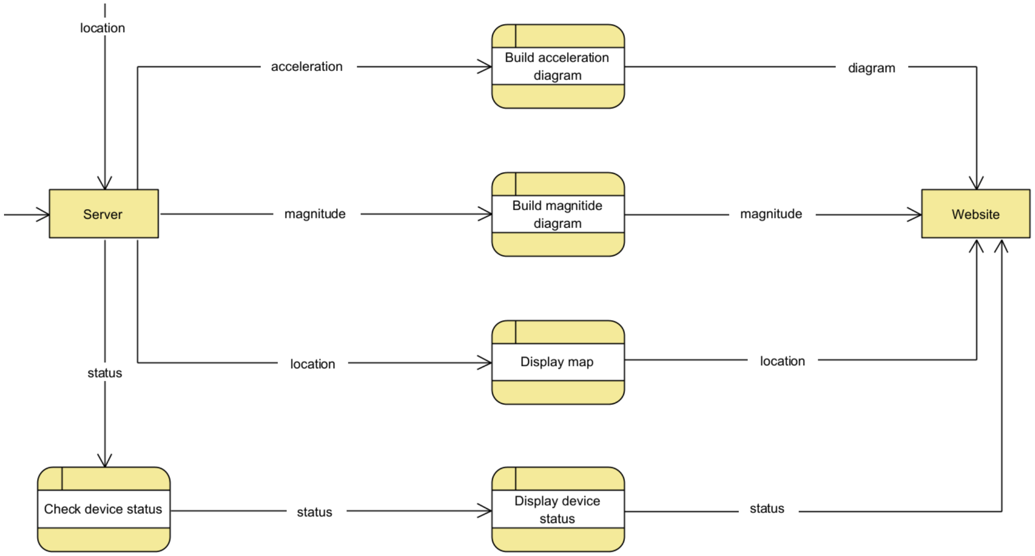
Data-flow diagram:

Our data-flow diagram consists of two parts: one from the sensors to the server, and one from the server to the website.



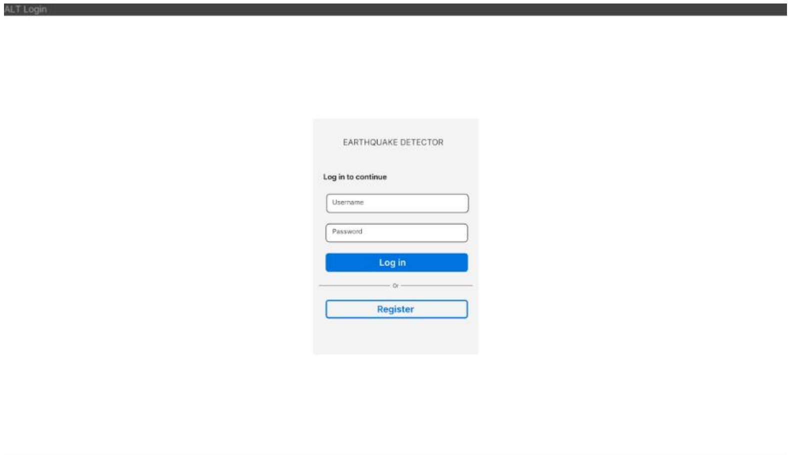
The first part of the data-flow diagram describes how the data is collected from various module and is calculated. For data collecting, we have two main modules: accelerometer and the GPS module. The accelerometer measures the gyro angle and the acceleration of the device. These measurements will be used in the calculation of magnitude in the scale of richter. Once the magnitude is calculated, it will be displayed along with the acceleration and gyro angle on the LCD screen. The magnitude and the acceleration will be uploaded to the server in a fixed interval. Meanwhile, the GPS module will locate the device and upload its location to the website. Additionally, if the alert is triggered, all the seismic activity (magnitude, acceleration) along with the location and timestamp will be logged and stored locally on the device.

The second part of the diagram visualizes how the data received from the device will be used on the server and the website. Once the server receives the acceleration and the magnitude statistics, it will draw their respective graphs (bar chart, line graph, etc.). The location will be used in displaying an interactive

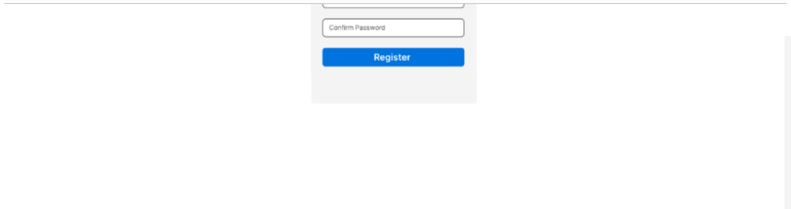


map, which will also display other devices if you have additional and also location taken from 3rd party APIs. Additionally, the server also frequently checks the device status to display on the website.

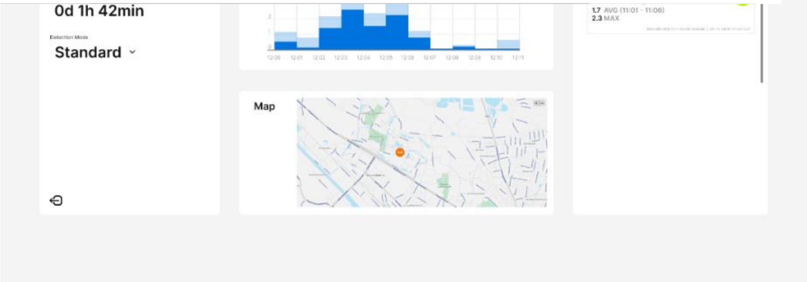
4. Product User Interface



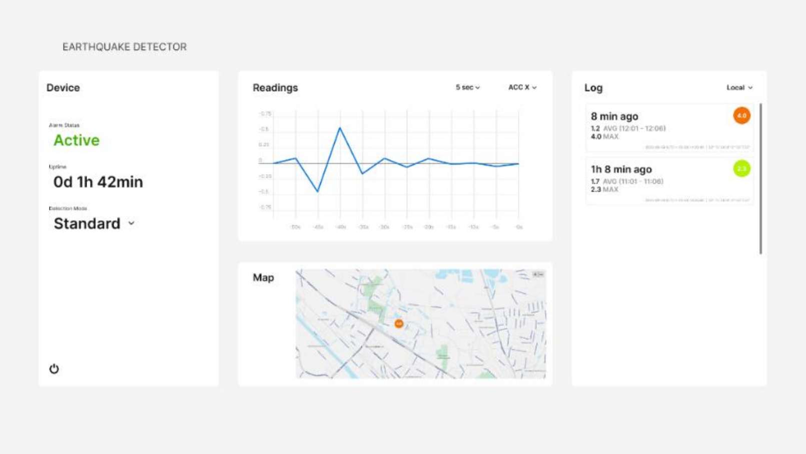
This is the first page that comes up when the website is opened. User either logs in with their own credentials or presses on register to get themselves registered with the device ID, e-mail, and password.



On the register interface, user enters their device’s ID, username, password, and confirmation of the password. After they are done with the credentials, they can press the register button on the bottom. If they would like to go back to log in screen, they can press the arrow which is on the top-left corner of the window.



After logging in users are greeted with a dashboard-style interface. The design is intentionally made simple and straightforward, so that the user can get the most important information at a glance. By default, the graph in the centre displays the average magnitude of the seismic activity over some time step (that the user is able to choose). The lighter blue represents the peak magnitude at that time. This graph can also display the acceleration on the device in the X, Y or Z direction. Below the graph is a map which shows the location of the device; the map is also overlaid with earthquake API data (points in the map for recent earthquakes). Left of that there is some basic information on the device: whether the alarm is armed, the uptime of the detector as well as the current detection profile (and other profiles in the dropdown menu).



EARTHQUAKE DETECTOR

Device

Alarm Status
Active

Uptime
0d 1h 42min

Detection Mode
Standard

Readings 5 sec ACC X

Log Local

8 min ago
1.2 AVG (12:01 - 12:06)
4.0 MAX

1h 8 min ago
1.7 AVG (11:01 - 11:06)
2.3 MAX

Map

On the right of the central graph there is a log of recent highlihted events (points where the readings exceeded the earthquake threshold). They display the the average magnitude for a 5 min interval around the point that triggered the alarm, as well as the maximim magnitude in that interval. The time and location are also noted. The log can also display global earthquake highlights harvested from the aforementioned API in similar format to the local data. You can switch between local/global data in the top right. Also, for convinience clicking on a point in the map will highlight you the relelvant log entry on the right.

5. Prevention/Mitigation Criteria (Security Controls)

- The data that is being collected should be reliable. The physical design should alllow the device to be fastened to a surface to minimize the chance of accidentaly moving the device and/or someone intentionally shaking it.
- To increase the reliablility of the device, the detection algorithm should account for accidental/intentional false data. One possible way is by taking into account the persistance of the elevated readings (for how long the device actively shakes – human made shaking tends to be shorter in duration).
- Access to sensitive device readings via the interface must be secured using username and password authentication. To further increase the security the stored passwords must be hashed (with bcrypt or Argon2) and salted. Other password-related basic security measures such as password security requirements, brute-force protection, etc. are also essential.
- A device can not be linked to more than one account. This deals with complexity of permissions and makes it harder for unauthorised user to accsess the device. This is because if the divice is linked to one account it wil automaticly block all other acounts from trying to accsess is, thus making it more secure.
- The website should be able to prevent injection or scripting attacks such as XSS attacks or SQL injection in the text input areas.

6. The cost involved (if any):

- Creating a secure case might take up to 6 hours of work and at least 2 hours to 3D print in DesignLab at no monetary cost; this might require more than one attempt if we aggree on a redisign or a mistake is made.
- Implementing a basic detection algorithm should not take longer than an hour, but having it be reliable and accurate will take additional research, testing and reiterations, so at least 7 – 20 hours over 2 sprints.
- Implementing the above mentioed security measures for passwords and securing the interface against common web attacks should take at least 5 hours, possibly quicker since most team members have experience with this from the previous module.
- Implementing linking the device with an account will take around 2 hours, assuming functioning components. On startup, the device will check if it has an ID, if not, it will generate one and display it on the LCD screen. Then, a user can use that ID when registering on the web interface and their log in credentials are saved on the server.

7. Conclusion:

*(You should give the **concluding remarks** of your document. You can do this by **highlighting noteworthy design decisions** and **challenges** for the next phase that you recognized.)*

As group 15, we have agreed to link device(s) to single account to reduce the security problem to the very least. For the reliability of the raw data that is being collected with the accelerometer, a physical case implementation has been the verdict after several discussions about the solution. We have agreed on the user-interface of the website as it was explained.

Reference:

*(Utilize this section to mention the **research papers/articles** you referred to for the document.)*

- NATO Advanced Research Workshop on Earthquake Monitoring and Seismic Hazard Mitigation in Balkan Countries (2005: Borovet͡s, Bulgaria), & Husebye, E. S. (2008). *Earthquake monitoring and seismic hazard mitigation in balkan countries: proceedings of the nato advanced research workshop on earthquake monitoring and seismic hazard mitigation in balkan countries, borovetz, bulgaria, 11-18 september 2005* (Ser. NATO science series. 4, earth and environmental sciences, v. 81). Springer. Retrieved September 13, 2023
- International Conference on Earthquake Engineering and Structural Dynamics (2017: Reykjavik, Iceland). (2019). Proceedings of the international conference on earthquake engineering and structural dynamics. (R. Rupakhety, S. Olafsson, & B. Bessason, Eds.) (Ser. Geotechnical, geological and earthquake engineering, volume 47). Springer. https://doi.org/10.1007/978-3-319-78187-7
- NATO Advanced Research Workshop on Earthquake Monitoring and Seismic Hazard Mitigation in Balkan Countries (2005: Borovet͡s, Bulgaria), & Husebye, E. S. (2008). Earthquake monitoring and seismic hazard mitigation in Balkan countries: proceedings of the NATO advanced research workshop on earthquake monitoring and seismic hazard mitigation in Balkan countries, Borovetz, Bulgaria, 11-18 September 2005 (Ser. Nato science series. 4, earth and environmental sciences, v. 81). Springer. Retrieved September 18, 2023